Please type a plus sign (+) inside this box → ☐ +

PTO/SB/21 (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/628,729
Filing Date	July 28, 2003
First Named Inventor	Eisentraeger
Group Art Unit	2131
Examiner Name	
Attorney Docket Number	MS1-1280US
Total Number of Pages in This Submission	

ENCLOSURES *(check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☑ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53

- ☐ Assignment Papers *(for an Application)*
- ☐ Drawing(s) Sheets
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) ________

- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group (*Appeal Notice, Brief, Reply Brief)*
- ☐ Proprietary Information
- ☐ Status Letter
- ☑ Other Enclosure(s) *(please identify below)*:

PTO-1449; 10 Non-Patent References; Return Receipt Postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	Thomas A. Jolly, Reg. No. 39,241
Signature	
Date	3/17/2004

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this date: March 17, 2004

Typed or printed name	Michelle G. Trujillo		
Signature	Michelle Trujillo	Date	3·17·04

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No.	10/628,729
Filing Date	Jul 28, 2003
Inventorship	Eisentraeger
Applicant	Microsoft Corporation
Attorney's Docket No.	MS1-1280US

Title: **Improved Tate Pairing Techniques for use with Hyperelliptic Curves**

INFORMATION DISCLOSURE STATEMENT

References -- See Attached Form PTO-1449

REMARKS

The citations listed, copies attached, are submitted in compliance with the duty of disclosure defined in 37 CFR §1.56. The Examiner is requested to make these citations of official record in this application.

Respectfully Submitted,

Date: 3/17/2004

By:
Thomas A. Jolly
Reg. No. 39,241

Please type a plus sign (+) inside this box → +

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1	of	1

Complete if Known

Application Number	10/628,729
Filing Date	July 28, 2003
First Named Inventor	Eisentraeger
Group Art Unit	Not Yet Assigned
Examiner Name	Not Yet Assigned
Attorney Docket Number	MS1-1280US

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		EISENTRAGER, KIRSTEN et al., "Fast Elliptic Curve Arithmetic and Improved Weil Pairing Evaluation," Topics in Cryptology, CT-RSA 2003, Marc Joye (Ed), pp. 343-354, LNCS 2612, Springer-Verlag, 2003.	
		BONEH, DAN, et al., "Identity-Based Encryption from the Weil Pairing," SIAM J. COMPUT., Vol 32, No. 3, pp. 586-615, 2003 Society for Industrial and Applied Mathematics.	
		MENEZES, ALFRED J., et al., "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," (0018-9448/93 1993 IEEE, IEEE Transactions on Information....), 8 pages.	
		FREY, GERHARD et al., "A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves," Mathematics of Computation, Vol. 62, No. 206, April 1994, pp. 865-874.	
		HESS, FLORIAN et al., "Two Topics in Hyperelliptic Cryptography," S. Vaudenay & A. Youssef (Eds.): SAC 2001, LNCS 2259, pp. 181-189, 2001.	
		BONEH, DAN, et al., "Short signatures from the Weil pairing," pp. 1-17.	
		GALBRAITH, STEVEN D. et al., "Implementing the Tate Pairing," Mathematics Dept., Royal Holloway, University of London, Egham, Surrey, UK & Hewlett-Packard Laboratories, Bristol, Filton Road, Stoke Gifford, Bristol, UK, pp. 1-14.	
		CANTOR, DAVID G., "Computing in the Jacobian of a Hyperelliptic Curve," Mathematics of Computation, Vol. 48, No. 177, January 1987, pp. 95-101.	
		BARRETO, PAULO S.L.M., et al., "Efficient Algorithms for Pairing-Based Cryptosystems," Universidade de Sao Paulo, Escola Politecnica, Sao Paulo (SP), Brazil & Computer Science Department, Stanford University, USA, pp. 1-16.	
		JOUX, ANTOINE, "The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems (Survey),"C. Fieker and D.R. Kohel (eds.): ANTS 2002, LNCS 2369, pp. 20-32, 2002 (Springer-Verlag Berlin Heidelberg 2002).	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.